IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): An image forming apparatus connectable to an external apparatus that enciphers and sends digital data including data intended to be printed and a program used by the image forming apparatus, said image forming apparatus comprising:

a key generating part configured to generate an enciphering key in response to a request from the external apparatus;

a storage part configured to store the enciphering key generated by the key generating part;

a key sending part configured to send the enciphering key to the external apparatus;

a deciphering part configured to decipher data received from the external apparatus, based on the enciphering key stored in the storage part;

a validity determining part configured to determine whether or not the deciphered data obtained by the deciphering part is valid;

a judging part configured to judge whether the deciphered data obtained by the deciphering part is for printing or for updating ~~and whether or not deciphered data obtained by the deciphering part is valid~~;

a printing part configured to print the deciphered data on a recording medium after the validity determining part determines that the deciphered data is valid and the judging part judges that the deciphered data ~~is valid and~~ is for printing; and

a processing part configured to update a version of the program used by the image forming apparatus based on the deciphered data after the validity determining part determines that the deciphered data is valid and the judging part judges that the deciphered data ~~is valid,~~

is for updating and includes data for updating the version of the program used by the image forming apparatus.

Claim 2 (Previously Presented): The image forming apparatus as claimed in claim 1, further comprising:

a request generating part configured to request the enciphered data with respect to the external apparatus.

Claim 3 (Canceled).

Claim 4 (Previously Presented): The image forming apparatus as claimed in claim 1, wherein said key generating part generates the enciphering key based on information peculiar to the image forming apparatus.

Claim 5 (Previously Presented): The image forming apparatus as claimed in claim 1, wherein said key generating part generates the enciphering key based on information peculiar to the image forming apparatus and a random variable.

Claim 6 (Currently Amended): An image forming apparatus connectable to an external apparatus that enciphers and sends digital data including data intended to be printed and a program used by the image forming apparatus, said image forming apparatus comprising:

a key generating part configured to generate an enciphering key in response to a request from the external apparatus;

a storage part configured to store the enciphering key generated by the key generating part;

a key sending part configured to send the enciphering key to the external apparatus;

a deciphering part configured to decipher data received from the external apparatus, based on the enciphering key stored in the storage part;

a validity determining part configured to determine whether or not the deciphered data obtained by the deciphering part is valid;

a judging part configured to judge whether the deciphered data obtained by the deciphering part is for printing or for updating ~~and whether or not deciphered data obtained by the deciphered part are valid~~; and

a processing part configured to update a version of a program used by the image forming apparatus based on the deciphered data after the validity determining part determines that the deciphered data is valid and the judging part judges that the deciphered data ~~is valid,~~ is for updating and includes data for updating the version of the program used by the image forming apparatus.

Claim 7 (Previously Presented): The image forming apparatus as claimed in claim 6, further comprising:

a request generating part configured to request the enciphered data with respect to the external apparatus.

Claim 8 (Canceled).

Claim 9 (Previously Presented): The image forming apparatus as claimed in claim 6, wherein said key generating part generates the enciphering key based on information peculiar to the image forming apparatus.

Claim 10 (Previously Presented): The image forming apparatus as claimed in claim 6, wherein said key generating part generates the enciphering key based on information peculiar to the image forming apparatus and a random variable.

Claim 11 (Currently Amended): An enciphered data processing method comprising:

a requesting step requesting data including data intended to be printed and a program used by an apparatus, with respect to a server;

a transmitting step enciphering requested data in the server and transmitting enciphered data via a network;

a deciphering step receiving and deciphering the enciphered data in the apparatus which at least has a printing function;

a validity determining part configured to determine whether or not the deciphered data obtained by the deciphering part is valid;

a judging step judging, in the apparatus, whether the deciphered data obtained by the deciphering part is for printing or for updating ~~and whether or not deciphered data obtained by deciphering the enciphered data in the deciphering step are valid~~;

a printing step printing the deciphered data on a recording medium in the apparatus after the validity determining part determines that the deciphered data is valid and the judging step judges that the deciphered data ~~are valid and are~~ is for printing; and

a processing step updating a version of a program used by the apparatus based on the deciphered data after the validity determining part determines that the deciphered data is

valid and the judging step judges that the deciphered data ~~are~~ is ~~valid, are~~ for updating and ~~include~~ includes data for updating the version of the program used by the apparatus.

Claim 12 (Previously Presented): The enciphered data processing method as claimed in claim 11, further comprising:

a request generating step requesting the enciphered data with respect to the server.

Claim 13 (Original): The enciphered data processing method as claimed in claim 12, wherein said request generating step generates the request from a terminal equipment which is coupled to the apparatus and is capable of accessing the server.

Claim 14 (Original): The enciphered data processing method as claimed in claim 12, wherein said request generating step generates the request from the apparatus which is capable of accessing the server.

Claim 15 (Previously Presented): The enciphered data processing method as claimed in claim 11, further comprising:

a key generating step generating an enciphering key which is used by said transmitting step and said deciphering step, in the apparatus.

Claim 16 (Original): The enciphered data processing method as claimed in claim 15, wherein said key generating step generates the enciphering key based on information peculiar to the apparatus.

Claim 17 (Original): The enciphered data processing method as claimed in claim 15, wherein said key generating step generates the enciphering key based on information peculiar to the apparatus and a random variable.

Claim 18 (Currently Amended): An enciphered data processing method comprising:

a requesting step requesting data including data intended to be printed and a program used by an apparatus, with respect to a server;

a transmitting step enciphering requested data in the server and transmitting enciphered data via a network;

a deciphering step receiving and deciphering the enciphered data in the apparatus which at least has a printing function;

a validity determining part configured to determine whether or not the deciphered data obtained by the deciphering part is valid;

a judging step judging, in the apparatus, whether the deciphered data obtained by the deciphering part is for printing or for updating ~~and whether or not deciphered data obtained by deciphering the enciphered data in the deciphering step are valid~~; and

a processing step updating a version of a program used by the apparatus based on the deciphered data after the validity determining part determines that the deciphered data is valid and the deciphered data is judged as ~~being valid and~~ for updating by the judging step and includes data for updating the version of the program used by the apparatus.

Claim 19 (Previously Presented): The enciphered data processing method as claimed in claim 18, further comprising:

a request generating step requesting the enciphered data with respect to the server.

Claim 20 (Original): The enciphered data processing method as claimed in claim 19, wherein said request generating step generates the request from a terminal equipment which is coupled to the apparatus and is capable of accessing the server.

Claim 21 (Original): The enciphered data processing method as claimed in claim 19, wherein said request generating step generates the request from the apparatus which is capable of accessing the server.

Claim 22 (Previously Presented): The enciphered data processing method as claimed in claim 18, further comprising:

a key generating step generating an enciphering key which is used by said transmitting step and the deciphering step, in the apparatus.

Claim 23 (Original): The enciphered data processing method as claimed in claim 22, wherein said key generating step generates the enciphering key based on information peculiar to the apparatus.

Claim 24 (Original): The enciphered data processing method as claimed in claim 22, wherein said key generating step generates the enciphering key based on information peculiar to the apparatus and a random variable.

Claim 25 (Currently Amended): An enciphered data processing system comprising:

a requesting part configured to request data including data intended to be printed and a program used by an apparatus, with respect to a server;

a transmitting part configured to encipher requested data in the server and transmitting enciphered data via a network;

a deciphering part configured to receive and decipher the enciphered data in the apparatus which at least has a printing function;

a validity determining part configured to determine whether or not the deciphered data obtained by the deciphering part is valid;

a judging part configured to judge, in the apparatus, whether the deciphered data obtained by the deciphering part is for printing or for updating ~~and whether or not deciphered data obtained by deciphering the enciphered data in the deciphering part are valid~~;

a printing part configured to print the deciphered data on a recording medium in the apparatus after the validity determining part determines that the deciphered data is valid and the judging part judges that the deciphered data ~~are valid and are~~ is for printing; and

a processing part configured to update a version of a program used by the apparatus in the apparatus based on deciphered data after the validity determining part determines that the deciphered data is valid and the judging part judges that the deciphered data ~~are valid, are~~ is for updating and ~~include~~ includes data for updating the version of the program used by the apparatus.

Claim 26 (Previously Presented): The enciphered data processing system as claimed in claim 25, wherein said requesting part is provided in a terminal equipment which is coupled to the apparatus and is capable of accessing the server.

Claim 27 (Previously Presented): The enciphered data processing system as claimed in claim 25, wherein said requesting part is provided in the apparatus which is capable of accessing the server.

Claim 28 (Previously Presented): The enciphered data processing system as claimed in claim 25, further comprising:

a key generating part configured to generate an enciphering key which is used by said transmitting part, in the apparatus.

Claim 29 (Currently Amended): An enciphered data processing system comprising:

a requesting part configured to request data including data intended to be printed and a program used for an apparatus, with respect to a server;

a transmitting part configured to encipher requested data in the server and to transmit enciphered data via a network;

a deciphering part configured to receive and decipher the enciphered data in the apparatus which at least has a printing function;

a validity determining part configured to determine whether or not the deciphered data obtained by the deciphering part is valid;

a judging part configured to judge, in the apparatus, whether the deciphered data obtained by the deciphering part is for printing or for updating ~~and whether or not deciphered data obtained by deciphering the enciphered data in the deciphering part are valid~~; and

a processing part configured to update a version of a program used by the apparatus based on deciphered data after the validity determining part determines that the deciphered data is valid and the deciphered data is judged as ~~being valid and~~ for updating by the judging part and includes data for updating the version of the program used by the apparatus.

Claim 30 (Previously Presented): The enciphered data processing system as claimed in claim 29, wherein said requesting part is provided in a terminal equipment which is coupled to the apparatus and is capable of accessing the server.

Claim 31 (Previously Presented): The enciphered data processing system as claimed in claim 29, wherein said requesting part is provided in the apparatus which is capable of accessing the server.

Claim 32 (Previously Presented): The enciphered data processing system as claimed in claim 29, further comprising:

a key generating part configured to generate an enciphering key which is used by said transmitting part, in the apparatus.

Claim 33 (Previously Presented): The image forming apparatus as claimed in claim 1, further comprising:

a notifying part configured to notify a result of printing by the printing part to the external apparatus.

Claim 34 (Previously Presented): The image forming apparatus as claimed in claim 1, further comprising:

a notifying part configured to notify the external apparatus when the judging part judges that the deciphered data are not valid.

Claim 35 (Previously Presented): The image forming apparatus as claimed in claim 1, further comprising:

a notifying part configured to notify completion of deciphering of the enciphered data by the deciphering part to the external apparatus so as to trigger an accounting process of the external apparatus.

Claim 36 (Previously Presented): The image forming apparatus as claimed in claim 1, further comprising:

a receiving part configured to receive thumbnails or summaries from the external apparatus; and

a selecting part configured to select a thumbnail or summary from the received thumbnails and summaries, and to send the selected thumbnail or summary to the external apparatus together with the enciphering key from the key sending part.

Claim 37 (Cancelled).

Claim 38 (Previously Presented): The enciphered data processing system as claimed in claim 25, further comprising:

an accounting part configured to carry out an accounting process with respect to the enciphered data after the enciphered data are transmitted to the apparatus.

Claim 39 (Previously Presented): The enciphered data processing system as claimed in claim 29, further comprising:

an accounting part configured to carry out an accounting process with respect to the enciphered data after the enciphered data are transmitted to the apparatus.